

Method and apparatus for geometric key establishment protocols based on topological groups

Abstract

The present invention proposes a continuous multi-parameter version of Diffie–Hellman protocol based on topological groups. In its turn, based on this continuous protocol, a method for public establishment and distribution of keys for encryption systems is implemented. An embodiment of the method, while providing an extremely high security level, is several orders of magnitude faster than the existing key establishment systems.